

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
information associated with the INSTAGRAM ID NUMBER)
[5ivepoint.marr (Instagram ID: 1819618354] which is stored at premises)
owned, maintained, controlled, or operated by Meta Platforms, Inc., a)
company headquartered at 1 Meta Way, Menlo Park, California, 94025.)
)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 4/12/2024

(not to exceed 14 days)

in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ Honorable Nancy Joseph
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

for days (not to exceed 30) until, the facts justifying, the later specific date of

Date and time issued: 3/29/2024 @ 1:08 p.m.

the later specific date of _____


Nancy Joseph
Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the **INSTAGRAM ID NUMBER**, below, which is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1 Meta Way, Menlo Park, California, 94025.

1. 5ivepoint.marr (Instagram ID: 1819618354)

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta Platforms, Inc. (“Meta”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in **Attachment A**:

- (a) All contact and personal identifying information, including **for user ID**: full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Instagram activities from **July 1, 2022, through February 5, 2024**.
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from **July 1, 2022, through February 5, 2024**, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos.
- (d) All profile information; status updates; videos, photographs, articles, and other items; Notes, friend lists, including the friends’ Instagram user identification numbers; groups and networks of which the user is a member, including the groups’ Instagram group identification numbers; future and past event postings; rejected

“Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Instagram applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.
- (f) All other records and contents of communications and messages made or received by the users from **July 1, 2022, through February 5, 2024**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “Friend” requests.
- (g) All “check ins” and other location information.
- (h) All IP logs, including all records of the IP addresses that logged into the account.
- (i) All records of the account’s usage of the “Like” feature, including all Instagram posts and all non- Instagram webpages and content that the user has “liked”.
- (j) All information about the Instagram pages that the account is or was a, “fan,” of.
- (k) All past and present lists of friends created by the account.
- (l) All records of Instagram searches performed by the account from **July 1, 2022, through February 5, 2024**,
- (m) The types of service utilized by the user.
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

- (o) All privacy settings and other account settings, including privacy settings for individual Instagram posts and activities, and all records showing which Instagram users have been blocked by the account.
- (p) All records pertaining to communications between Instagram and any person regarding the user or the user's Instagram account, including contacts with support services and records of actions taken.
- (q) Instagram is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. 1709 (Mail Theft) involving Damari Johnson since July 1, 2022, including, the user ID identified on Attachment A, information pertaining to the following matters:

- (a) The purchase, sale, and possession of stolen checks,
- (b) Photographs of Damari Johnson and associates.
- (c) Any information concerning mail, bank accounts, checks, burglaries, robberies,
- (d) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner.
- (e) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation.
- (f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

Case No. 24-845M(NJ)

information associated with the INSTAGRAM ID NUMBER [5ivepoint.marr (Instagram ID: 1819618354] which is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1 Meta Way, Menlo Park, California, 94025.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (*identify the person or describe the property to be seized*):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1709

Offense Description

The application is based on these facts:

Please see Affidavit.

Continued on the attached sheet.

Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Scott Zimmerman, Special Agent - USPS-OIG

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: 3/29/2024

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Scott Zimmerman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook or Instagram user ID that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), a social networking company headquartered at 1 Meta Way, Menlo Park, California, 94025. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Meta to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

2. I am a Special Agent with the United States Postal Service Office of Inspector General, (USPS-OIG), and have been so employed for approximately 2 years. The USPS-OIG is the primary investigative arm of the United States Postal Service for employee investigations and is charged under Title 18, United States Code, Section 3061 with the enforcement of laws governing the use and movement of the United States mail, including employee misuse and fraudulent schemes involving the mail, crimes relating to mail fraud, narcotics trafficking and identity theft. Previously, I was a United States Postal Inspector for approximately 5 years and a Federal Air Marshal for approximately 10 ½ years.

3. Throughout my employment as a Federal Agent, I have participated in the execution of search warrants involving searches and seizures of residences, businesses, and vehicles. These warrants often included the seizure of computers, cellular phones, related electronic equipment such as printers and laminators and requisite software to operate computers

and peripheral devices. I have participated in numerous complex narcotics, shootings, armed robbery, burglary, and assault investigations in violation of Title 18, United States Code, Sections 924(c), 2114, 2115, 111 and other related offenses.

4. The factual allegations set forth herein are based on my personal observations and knowledge, in addition to information obtained from other investigators, public and private records, cooperating witnesses and other involved parties and sources as indicated herein. Because this Affidavit is submitted for the limited purpose of demonstrating probable cause for the warrant sought, I have not included each and every fact known to me or other law enforcement officers about this investigation.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe a violation(s) of 18 U.S.C. 1709 (Mail Theft), has been committed by the individual identified below. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

6. The USPS-OIG is investigating employee Damari Johnson (Johnson), who is suspected of stealing checks from the U.S. Mail while conducting USPS duties. The case is related to a larger investigation and their associates.

7. A criminal enterprise known as the “Scamily,” Crew utilized Instagram to communicate with other members who may be involved with check washing operations. The Postal Inspection Service, Federal Bureau of Investigation (FBI), and Milwaukee Police Department (MPD) have conducted parallel investigations regarding this group and the use of firearms against USPS Carriers.

8. On or about January 3, 2024, fourteen non-postal employees were charged with 77 counts relating to robbery, mail theft, forgery, money laundering, racketeering, and continuing a criminal enterprise by the Milwaukee County District Attorney's Office, Case: 2024CF0034. MPD obtained suspect Hussein Abdurahman Haji's (Haji) Instagram account information as part of the State RICO investigation. MPD searched a cellular device belonging to Haji. This device held communications/chats/SMS displaying conspiracy to conduct check washing operations with a nexus to USPS Arrow keys and the theft of mail.

9. The criminal complaint states during MPD's investigation, a subpoena was drafted for Haji's Instagram and Facebook accounts. The accounts were identified from a search of Haji's phone which disclosed from January 2022 through the time of his arrest, Haji consistently conspired to cash fraudulent checks at banks and obtain items of value using other people's identifying information without their consent.

10. Affiant knows that analysis of Haji's phone showed that one Instagram account utilized by Hussein Haji was 2900scamily.sain (Instagram ID: 2543632723). The Milwaukee Area Violent Crime Task Force (MAVCTF), a joint law-enforcement task force which includes members of the FBI, Milwaukee Police Department, and United States Postal Inspection Service (USPIS), obtained account information, including communications to and from that account with other Instagram users, via federal search warrant in July of 2023. The FBI acquired Haji's Instagram account information as part of that federal Hobbs Act Robbery investigation.

11. During the search of Haji's "2900scamily.sain" account information, it was determined Johnson had communicated with Haji. Johnson and Haji communicated on Instagram about checks flowing through the mail. Johnson was not arrested nor charged in connection with the criminal enterprise.

12. On January 10, 2024, Inspector Massari informed the affiant of Johnson's potential involvement with the Scamily crew, because Inspector Massari discovered Johnson may be a USPS employee. Inspector Massari stated he was contacted by Milwaukee Police Detective Portnoy during the week of January 7, 2024, regarding the Instagram text messages referenced in this affidavit. Inspector Massari provided the affiant with copies of the Instagram messages he received from MPD involving Johnson.

13. The following are the Instagram handles/monikers related to this warrant...

- 2900scamily.sain (Instagram: 2543632723) is the Instagram handle which FBI investigation has shown to be controlled by the Hussein Haji.
- 5ivepoint.marr (Instagram: 1819618354) is the Instagram handle determined to be controlled by Damari Johnson.

14. Affiant has reviewed communications between the two accounts which were obtained by the federal search warrant return of the Instagram account of "2900scamily.sain". Those messages show the following:

- On November 3, 2022, 2900scamily.sain communicated with account "5ivepoint.marr." In those messages, 5ivepoint.marr sent a message containing phone number (414) 309-6821. Affiant cross referenced the phone number (414) 309-6821 on open-source Database CLEAR which the affiant has used in the past and found to be reliable. The CLEAR Database shows that number was utilized by postal employee Damari Johnson on or before November 3, 2022.

15. USPIS Inspector Massari further provided the affiant a transcript of Haji's Instagram page. A review of Haji's Instagram page revealed, starting on October 29, 2022, the Instagram handle, 2900scamily.sain communicated with Instagram handle 5ivepoint.marr on the

Instagram messaging platform. The Instagram chat conversations from October 28, 2022 to November 24, 2022, both accounts discussed with Chase bank accounts, sharing information related to suspected check washing operations, and obtaining checks from the U.S. Mail stream. The Instagram handle 5ivepoint.marr passed phone number, (414) 309-6821, as a good contact number to the Scamily Crew handle, 2900scamily.sain. The person using 5ivepoint.marr typed on November 22, 2022, “I work at the post office gng imao them bitches flow through every day.”

16. Phone number (414) 309-6821 was further queried through USPS databases and was listed under USPS Employee Damari Johnson’s profile. According to USPS databases Johnson was assigned as a mail handler at the USPS Oak Creek, WI Annex.

17. On February 5, 2024, Johnson was interviewed by Postal Inspector Chris Massari and the affiant at the Oak Creek, WI Annex. The interview was in response to Johnson’s accounts with the, “Scamily,” Instagram account, and the fact Johnson was still employed by the USPS. Prior to the interview the affiant advised Johnson of his Garrity Rights, verbally, which Johnson stated he understood. The interview was the first time Johnson was made aware he was under investigation. The following is related in summary and not verbatim.

18. Johnson was provided with a Fox News photo of the individuals identified in a news story as being part of the; “Scamily.” Johnson circled the 2 suspects he said he associates with and initialed the photo. Johnson identified the first suspect he circled on the left side of the photo as, “Hussein,” and the second suspect to the upper right of Hussein as, “Felix.” Johnson would not provide last names for either suspect. Johnson said he has known Felix and Hussein since childhood and went to school with them. Johnson vehemently denied having an affiliation with the, “Scamily,” crew.

19. Johnson explained the person he knows as Felix approached him between the August to November 2022 time frame regarding his employment with USPS and the suspected criminal operations the; “Scamily,” crew was conducting at the time. Johnson stated he never provided any U.S. Mail to this criminal enterprise. Johnson repeatedly explained he was not involved with the; “Scamily,” operation. Johnson said the people he recognized and knew who were involved with stolen U.S. Mail had nothing to do with him because he was not involved.

20. Johnson admitted to committing mail theft for approximately 9 months from August 2022 to May 2023. Johnson stated he looked for envelopes he thought contained checks while working as a mail handler at the Milwaukee Processing and Distribution Center (P&DC). Johnson said he only stole checks while he worked at the Milwaukee P&DC. Johnson could not remember exactly how many checks he stole, but estimated it was under 10 checks. Johnson estimated he transferred from the Milwaukee P&DC to the Oak Creek Annex in May of 2023.

21. Johnson stated if he saw what he believed to be a check, he would fold up the envelope and put it inside his pant pocket. Johnson could not remember the amounts the checks were written for. Johnson explained he took the checks to make quick money. Johnson described his actions as a, “back end money move.” Johnson stated he attempted to sell the checks online for money but was unsuccessful. Johnson could not remember what application or website he used when he attempted to sell the checks. Johnson denied cashing any of the stolen checks. Johnson said since he was unable to sell the stolen checks, he ripped them up and threw them away.

22. Johnson stated he acted alone, and it was his own personal decision to steal the checks. Johnson stated he does not know of any other employees at the Milwaukee P&DC or Oak Creek Annex committing mail theft.

23. Johnson stated he communicated with the; “Scamily,” crew using an Instagram account under the name 5ivepoint.marr (Instagram: 1819618354). Johnson was provided with a transcript of Instagram communications between the handles 5ivepoint.marr and 2900scamily.sain (Instagram: 2543632723) from November 22, 2022. Johnson read the transcript and acknowledged he was communicating with Hussein regarding his knowledge of checks processed through the U.S. Mail. Johnson said he was not paid by the, “Scamily,” crew but stated he should have charged them for the information he provided in the transcript. Johnson initialed and dated the Instagram transcript.

24. Johnson explained he routinely cancels his social media accounts and will start new accounts at various times. It is strongly suspected Hussein Abdurahman Haji was the main operator of 2900scamily.sain account. Hussein was one of the individuals who was arrested as part of the, “Scamily,” criminal enterprise. Johnson stated he corresponded with the, “Scamily,” account explaining, “I work at the post office gng lmao them bitches flow through every day. I’m lyk I can get em.” Johnson explained he responded to the Instagram posts to give the appearance of being involved in operations for representational purposes.

25. Johnson said the last time he spoke with Hussein was in early January 2024, when Hussein called him on his cell phone. Johnson reiterated he had nothing to do with the, “Scamily.” Although Johnson admitted communicating with the, “Scamily,” regarding his knowledge of checks flowing through the mail, Johnson denied providing the, “Scamily,” with checks or having any involvement or affiliation with them.

26. At the conclusion of the interview, Johnson declined to provide a sworn written statement. USPS management was briefed on the results of the interview at which time Johnson

was placed on USPS Emergency Placement. Johnson was put up for removal by USPS Management on March 15, 2024.

TECHNICAL INFORMATION

27. Meta Platforms, Inc. owns and operates the free-access social networking websites called Facebook and Instagram that can be accessed at <http://www.facebook.com> and <http://www.Instagram.com> respectively. Facebook/Instagram allow its users to establish accounts with Facebook/Instagram, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook/Instagram users, and sometimes with the general public.

28. Facebook/Instagram asks users to provide basic contact and personal identifying information to Facebook/Instagram, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook/Instagram passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook/Instagram also assigns a user identification number to each account.

29. Facebook/Instagram also collects and retains information about how each user accesses and uses Facebook/Instagram. This includes information about the IP addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

30. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the

primary account, can switch between the associated accounts on a device without having to repeatedly log in and log out.

31. Instagram users can also connect their Instagram and Facebook accounts to use certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account or transfer an image from Instagram to a connected image printing service. Facebook maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

32. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

33. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also

allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

34. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

35. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

36. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the

photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

37. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

38. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

39. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

40. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

41. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the

account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

42. Instagram users have several ways to search for friends and associates to follow on Instagram, such as by allowing Facebook to access the contact list on their devices to identify which contacts are Instagram users. Facebook retains this contact data unless deleted by the user and periodically syncs with the user’s devices to capture changes and additions. Users can similarly allow Facebook to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

43. Each Instagram user has a profile page where certain content they create and share (“posts”) can be viewed either by the general public or only the user’s followers, depending on the privacy settings. Users can customize their profile by adding their name, a photo, a short biography (“bio”), and a website address.

44. One of Instagram’s primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or store on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of others (“tag”), or add a location. These appear as posts on the user’s profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Facebook servers.

45. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are “tagged” in a post by its creator or mentioned in a comment (user can “mention” others by adding their username to a comment followed by “@”). An Instagram post created by one user may appear on

the profile or feeds of other users depending on several factors including privacy settings and which users were tagged or mentioned.

46. An Instagram “story” is like a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Story Archive” and remain on Facebook servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

47. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram’s long-form video app.

48. Instagram’s direct messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, profiles, and other information. Participants to a group conversation can name the group and send invitations to other to join. Instagram users can send individual or group messages with “disappearing” photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can’t view their disappearing messages after they are sent but do have access to each message status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

49. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform, Facebook, and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

50. Instagram has a search function which allows users to search for accounts by username, user activity by location and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be “followed” to generate related updates from Instagram. Facebook retains records of a user’s search history and followed hashtags.

51. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

52. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

53. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile and would show when and from what IP address the user did so.

54. Facebook collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Facebook to personalize and target advertisements.

55. Social networking providers like Meta Platforms, Inc. typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with

the service (including any credit card or bank account number). In some cases, Facebook or Instagram users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta Platforms, Inc. typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

56. As explained herein, information stored in connection with a Facebook or Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook or Instagram user's IP log, stored electronic communications, and other data retained by Meta Platforms, Inc., can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook or Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses; investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under

investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Lastly, Facebook or Instagram account activity may provide relevant insight into the Facebook/ Instagram account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook/ Instagram account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

57. Therefore, the computers of Meta Platforms, Inc. are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook/Instagram, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

58. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

59. Based on the foregoing, I request that the Court issue the proposed search warrant.

60. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta Platforms, Inc. Because the warrant will be served on Meta Platforms, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

61. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Eastern District of Wisconsin is a district court of the United States which has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

62. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

63. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the **INSTAGRAM ID NUMBER**, below, which is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1 Meta Way, Menlo Park, California, 94025.

1. 5ivepoint.marr (Instagram ID: 1819618354)

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta Platforms, Inc. (“Meta”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in **Attachment A**:

- (a) All contact and personal identifying information, including **for user ID**: full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Instagram activities from **July 1, 2022, through February 5, 2024**.
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from **July 1, 2022, through February 5, 2024**, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos.
- (d) All profile information; status updates; videos, photographs, articles, and other items; Notes, friend lists, including the friends’ Instagram user identification numbers; groups and networks of which the user is a member, including the groups’ Instagram group identification numbers; future and past event postings; rejected

“Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Instagram applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.
- (f) All other records and contents of communications and messages made or received by the users from **July 1, 2022, through February 5, 2024**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “Friend” requests.
- (g) All “check ins” and other location information.
- (h) All IP logs, including all records of the IP addresses that logged into the account.
- (i) All records of the account’s usage of the “Like” feature, including all Instagram posts and all non- Instagram webpages and content that the user has “liked”.
- (j) All information about the Instagram pages that the account is or was a, “fan,” of.
- (k) All past and present lists of friends created by the account.
- (l) All records of Instagram searches performed by the account from **July 1, 2022, through February 5, 2024**,
- (m) The types of service utilized by the user.
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

- (o) All privacy settings and other account settings, including privacy settings for individual Instagram posts and activities, and all records showing which Instagram users have been blocked by the account.
- (p) All records pertaining to communications between Instagram and any person regarding the user or the user's Instagram account, including contacts with support services and records of actions taken.
- (q) Instagram is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. 1709 (Mail Theft) involving Damari Johnson since July 1, 2022, including, the user ID identified on Attachment A, information pertaining to the following matters:

- (a) The purchase, sale, and possession of stolen checks,
- (b) Photographs of Damari Johnson and associates.
- (c) Any information concerning mail, bank accounts, checks, burglaries, robberies,
- (d) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner.
- (e) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation.
- (f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).